AMP-Algebra Tuesday Lecture 2

Binary operations & Groups

Yesterday we talked about set theory. Now sets are just bags of elements, and don't have any "structure". Like if we're thinking of the integers $\mathbb{Z}$ as just a set, there's nothing there to do "algebra" with. It's the structure of $\mathbb{Z}$, the operations of addition ($+$) and multiplication ($\cdot$) on $\mathbb{Z}$, that give us something to study algebraically. So let's talk about this idea of a set having structure (having an operation) defined on it more generally.

Define $S \times S = \{(x,y) \mid x \in S \; y \in S\}$

Definition

For a set S, a binary operation $*$ on S is a function $*: S \times S \to S$. So a binary operation takes two elements in your set and gives you some third element of your set.

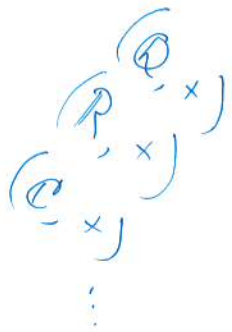
Yesterday we talked about functions being "well-defined". Well, a binary operation IS a function, so it too must be well-defined; so for $* : S \times S \to S$

- $*$ needs to be defined for every pair of elements in S. EVERY PAIR.
- If you define $*$ by some "rule" or "formula" you need to make sure that formula/rule actually gives you something back in S for every pair of elements in S.

Let's talk about some examples:

- Addition on $\mathbb{Z}$ is a binary operation, and so is multiplication.

$$+ : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z} \qquad \cdot : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$$
$$(a, b) \mapsto a+b \qquad (a, b) \mapsto a \cdot b$$



- For a non-example, consider the natural numbers $\mathbb{N} = \{1, 2, 3, \ldots\}$ and the operation of division. If you divide one natural number by another, the result might not be a natural number. $2 \div 3 \notin \mathbb{N}$ ∴

- For a goofier example, let S be the set of all colors, and for $a, b \in S$, let $a * b$ be the result of mixing together the colors a and b in equal parts. $a * b$ must be some well-defined color, so $* : S \times S \to S$ is a binary operation on S.

- A last, more abstract example: Think about how we can write down the "multiplication table" for $\mathbb{Z}$. ~~This~~ Doing this literally defines the binary operation of multiplication $*$ on $\mathbb{Z}$ by listing the products of all the elements explicitly. We can similarly define a binary operation explicitly like this on any set. So, let's take the set $S = \{a, b, c\}$.

$*$	a	b	c
a	b	c	b
b	a	c	b
c	c	b	a

a*b

b*c

b*a

$*$	a	b	c
a	c	a	b
b	a	b	c
c	b	c	a

Each of these define binary operations $*$ on S.

But ANY such table will define a valid binary operation. That's boring! This gives us hardly any structure at all! Naturally occurring binary operations though end up obeying some additional RULEZ. Let's look back to our faverite set $\mathbb{Z}$ so I can point out some of these rules. So consider $\mathbb{Z}$ equipped with the binary operation of addition $(+)$. Remember that $(+)$ obeys these rules:

(1) Addition is <u>associative</u>. For example

$$2+(3+5) = (2+3)+5$$

(2) $\mathbb{Z}$ with $(+)$ has an <u>identity element</u> called zero (0) with the property that

$$0+x = x+0 = x \quad \text{for any } x \in \mathbb{Z}.$$

(3) Every element x of $\mathbb{Z}$ has an <u>inverse element</u>, specifically named $-x$ in $\mathbb{Z}$ under $(+)$, such that $x+(-x)=0$.

Now we could have picked ANY rules to inspire how we proceed, but classically, we, and every single textbook on abstract algebra, starts with these rules, and with the study of the following algebraic structures.

Definition

We'll say a set G equipped with a binary operation $(*)$ is a group if $(*)$ obeys the following:

(1) $*$ is associative: $a*(b*c) = (a*b)*c$ $\forall a,b,c \in G$ ("for all")

(2) G has some identity element, usually named e, with respect to $*$. So for all $a \in G$, $a*e = e*a = a$.

(3) Every element $a \in G$ has an inverse, an element generally denoted $a^{-1} \in G$, such that $a*a^{-1} = a^{-1}*a = e$. (just notation though)

A few notes about this definition: If we're talking about a group we "should" always denote it as $(G, *)$ because both the set G and operation $(*)$ are necessary to define the group... but often we'll get sloppy and just write G for the group and leave the operation $(*)$ implied.

The identity element is usually called "e" for the German word "einheit", which translates to something like the word "unit".

Now let's give some examples of groups! 

- $(\mathbb{Z}, +)$ is a group with identity element 0, and every element x has an inverse $-x$.

- Let S be the set of real numbers excluding zero. S is a group under multiplication, since multiplication is associative, 1 is an identity under multiplication, and every $s \in S$ has a multiplicative inverse $\frac{1}{s} \in S$ such that $s \times \frac{1}{s} = \frac{1}{s} \times s = 1$.

- And, like before, we can define a group by listing out what the binary operation does explicitly. For $S = \{a, b, c\}$ you can define a group structure on S with $(*)$ via

$*$	a	b	c
a	c	a	b
b	a	b	c
c	b	c	a

Question

What is the identity element of this group $(S, *)$? For each element of the group can you identify its inverse? Finally, can you confirm that $(*)$ is associative, thus confirming $(S, *)$ really is a group?